

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-18. (canceled)

19. (currently amended) A group signature device for providing a message (m) accompanied by a group signature (S), comprising:

means for storing personalized data (z, Kz) identifying [[an]]any one individual member (M) of a group (G), wherein said group signature device is associated to said one individual member (M) of the group (G);

means for storing a predefined private signature key (SK) common to all members of the group (G);

encryption means (B3) for producing [[an]] a single encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz) of [[one]]said one individual member (M) only;

signing means (B6) ~~for producing~~which enables said one individual member (M) to produce the group signature (S) on behalf of the group (G) with ~~using said stored predefined~~ private signature key (SK) common to all group members, ~~using wherein only~~ the message to be signed (m) and said single encrypted text (C) produced using the personalized data (z, Kz) of said one individual member (M) ~~only~~are used to produce said group signature (S); and

means for outputting the message (m) and the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that the message (m) is associated with the group (G) based

on the group signature (S), with the identity of the individual member (M) of the group (G) remaining anonymous to the checker.

Claim 20. (canceled)

21. (previously presented) A group signature device according to claim 19, further comprising:

means (B5) for combining the message (m) to be signed and the encrypted text (C) in the form of a concatenation of the message (m) with the encrypted text (C).

Claim 22. (canceled)

23. (previously presented) A group signature device according to claim 19, wherein

said personalized data is an identifier (z) personal to the individual member (M);

said means for storing further includes an encryption key (K) common to all members of the group (G); and

encryption means (B3) produces said encrypted text (C) using the identifier (z) and said encryption key (K).

24. (previously presented) A group signature device according to claim 23, in which encryption means (B3) produces said encrypted text (C) using the identifier (z) and a random number (r).

25. (previously presented) A group signature device according to claim 19, wherein

said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G); and

encryption means (B3) produces said encrypted text (C) using at least one data and said diversified encryption key (Kz).

26. (previously presented) A group signature device according to claim 25, wherein said at least one data includes a random number (r).

27. (previously presented) A group signature device according to claim 19, wherein the encryption means (B3) uses a secret key encryption algorithm.

28. (previously presented) A group signature device according to claim 19, wherein the encryption means (B3) uses one of the Rivest, Shamir, Adleman (RSA) public key encryption algorithm or the Advanced Encryption Standard (AES) secret key encryption algorithm.

29. (previously presented) A group signature device according to claim 19, wherein the signing means (B6) uses a private key signature algorithm (SK).

30. (previously presented) A group signature device according to claim 29, in which the private key signature algorithm is of the Rivest, Shamir, Adleman (RSA) type.

31. (previously presented) A group signature device according to claim 19, in which said group signature device is a portable communicating device.

32. (previously presented) A group signature device according to claim 31, in which said portable communicating device is a smart card.

33. (currently amended) A method for secure communication of message (m) sent by ~~any one~~ individual member (M) of a group (G) using a group signature (S), said method comprising:

storing, using a group signature device, personalized data (z, Kz) that identifies said one individual member (M) of the group (G);

storing, using the group signature device, a predefined private signature key (SK) that is common to all members of the group (G);

producing, by said one individual group member (M), the group signature (S) of the message (m) on behalf of the group (G) by signing, with [[a]]said predefined private signature key (SK) common to all group members stored on said group signature device, a set including the message (m) and a single encrypted text (C) produced using a personalized data (z, Kz) of said one individual member (M) only; and

outputting the message (m) along with the group signature (S).

34. (previously presented) The method according to claim 33, further comprising:

verifying, by using a public key (PK) corresponding to said private signature key (SK), that the message (m) is associated with the group (G) based on the group signature (S), without identifying the individual member (M) of the group (G).

35. (previously presented) The method according to claim 33, further comprising the steps of:

decrypting the encrypted text (C) thus obtaining the personalized data (z, Kz); and identifying the individual member (M) of the group (G) based on said personalized data (z, Kz).

36. (currently amended) The method of claim 35, further comprising:

producing [[a]]said predefined private signature key (SK) common to all members of group (G);

producing personalized data (z, Kz) identifying the individual member (M) accepted into the group (G); and

registering said personalized data (z, Kz) with the private signature key (SK) in an electronic device personalized to said individual member (M) of the group (G).

Claims 37-38. (canceled)

39. (currently amended) A group signature system associated to any one individual member (M) of a group (G) and configured for -ensuring a secure communication of a message (m) sent by [[an]]said one individual member (M) of [[a]]the group (G) using a group signature (S), said group signature system comprising:

an electronic device configured to store a personalized data (z, Kz) identifying said one [[said]] individual member (M) of the group (G), to store a predefined private signature key (SK) that is common to all members of the group (G), to produce [[an]]a single encrypted text (C) intended to be associated with said message (m) using said personalized data (z, Kz) of said one individual member (M), and to produce the group signature (S) with -a private signature key (SK) common to all group members using the message (m) and said single encrypted text (C) produced using the personalized data (z, Kz) of said one individual member (M) only, and to output the message (m) and the group signature (S);

a checker that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group (G) based on the group signature (S), the identity of the individual member (M) remaining anonymous to the checker; and

a trusted authority configured to identify the individual member (M) of the group (G).

Claim 40. (canceled)